REMARKS

This is in response to the Official Action mailed on April 5, 2007. Claims 1-23 were pending in that action and all claims were rejected. With the present response, claims 1 and 21 are amended and claim 2 is cancelled. Consideration and allowance of all pending claims are respectfully solicited in light of the following comments.

Beginning on page 2 and continuing for the remainder of the Office Action, claims 1-23 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,446,092 (hereinafter referred to as "the Sutter reference"). In general, the Sutter reference pertains to a distributed database system. The bulk of the reference is focused on describing the details of data management within the distributed system. Very little of the description has anything to do with database security. Even less of the description has to do with security issues relevant to Applicant's claims. There is, as is pointed out in the Office Action, some description of database security at least in columns 85-90 of the Sutter reference.

Independent claim 1, as presently amended, recites a method that includes receiving a password from a user. The password is utilized as a basis for generation of a user-specific version of an encryption component. As claimed, the encryption component is a collection of data that specifies an encryption or decryption process. Further, as claimed, a user is selectively allowed to process the user-specific version of the encryption component so as to derive the encryption component (emphasis added). Finally, as claimed, the encryption component is utilized to process sensitive data.

The Sutter reference discusses password processing in columns 89 and 90. In column 90, a regular user log-in process is described. In accordance with that process, an application requests a userID and password from the user. The application then passes the user-name, password and database information to a security library component. The security library component

transmits the information to a replication engine. The replication engine validates the received information and releases a set of keys to the security library component. If the user is not authenticated, the replication engine and the security library component report a log-in failure to the requesting application.

Notably, this process for logging in and authenticating a user in no way involves utilizing a received password as a basis for generation of a user-specific version of an encryption component as claimed. Of course, the step of selectively allowing a user to derive the encryption component from the user-specific version is also missing.

The Sutter reference also describes an administrator log-in process at column 89, lines 31-40. In accordance with this process, an administrator selects a password or pass-phrase from which a system component derives a key (e.g., by repeatedly hashing the pass-phrase). Notably, the key is then used to encrypt a key table that contains symmetric database encryption keys.

One might argue that the described administrator log-in process involves utilizing a user-specific version of an encryption component to process sensitive data. However, there is absolutely no teaching or suggestion of any process step similar to the claimed selectively allowing the user to process to the user-specific version of the encryption component so as to derive an encryption component that is utilized to process sensitive data. In accordance with the teachings of Sutter, an encrypted password is utilized as an encryption component for processing sensitive data. In contrast, claim 1 recites a method wherein the user-specific version is not used as the encryption component but is instead used as a selectively removable, user-specific

obfuscation of an encryption component for processing sensitive data.

For all of these reasons, it is respectfully submitted that independent claim 1 is patentably distinguishable from the cited Sutter reference. Reconsideration and allowance of claim 1 are respectfully solicited.

Dependent claims 3-13 are dependent upon independent claim 1 and are believed to be in allowable form at least for the same reasons outlined above in relation to that independent claim. Further, it is respectfully submitted that at least some of these dependent claims are patentable based on the merit of their own claim limitations. For example, dependent claim 7 adds a step of generating a second user-specific version of the encryption component. Notably, this means a second user-specific version of the same encryption component. This is in stark contrast to the Sutter administrator log-in process, which does not involve making different, user-specific versions of a common key. Claim 7 is but one example of a dependent claim that is believed to be in allowable form based on the merits of its own claim limitations.

Independent claim 14 recites a method that includes creating and storing a plurality of user-specific versions of an encryption component. As claimed, users are selectively allowed to process their version of the encryption component so as to derive the encryption component. The encryption component is then utilized to process sensitive data.

As was discussed above in relation to other pending claims, the Sutter reference, at best, teaches generating an encryption component based on a password. There is absolutely no teaching or suggestion of selectively allowing users to process their version of an encryption component so as to derive the encryption component. Further, there is absolutely no teaching or

suggestion of an encryption component derived as claimed and utilized to process sensitive data. For all of these reasons, it is respectfully submitted that independent claim 14 is in allowable form.

Dependent claims 15-20 are dependent upon independent claim 14 and are believed to be in allowable form for at least the same reasons discussed above in relation to that affiliated independent claim. Further, it is respectfully submitted that at least some of these dependent claims are in allowable form based on the merit of their own claim limitations. For example, dependent claim 15 further defines the step of storing a plurality of user-specific versions of an encryption component as storing the user-specific version in a user account for each of a plurality of users. A close examination of the passages cited by the Examiner against this dependent claim, as well as a close examination of the Sutter reference in its entirety, reveals that there is no teaching or suggestion of storage in user accounts as claimed. Claim 15 is but one example of a dependent claim believed to be allowable based on the merit of its own claim limitations.

Independent claim 21 and its affiliated dependent claims 22-23 pertain to a method that includes utilizing a password as a basis for decrypting a user-specific version of an encryption component. As claimed, the encryption component is a collection of data that specifies an encryption or decryption process. Further, as claimed, utilizing the password is contingent upon the encrypted version matching an authorized value and a successful check of allocated user access privileges.

It is respectfully submitted that the Sutter references absolutely fails to teach or suggest making utilization of a password to decrypt a user-specific version of an encryption component contingent upon an authorization and access privilege

analysis as claimed. For at least these reasons, it is respectfully submitted that claims 21-23 are in allowable form.

In summary, it is respectfully submitted that claims 1 and 3-23 are in condition for allowance. Reconsideration and allowance are respectfully requested. The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: _____

Christopher L. Holt, Reg. No. 45,844
900 Second Avenue South, Suite 1400
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

CLH:rkp